

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215255

(43)Date of publication of application : 04.08.2000

(51)Int.Cl.

G06F 19/00
// G09C 1/00

(21)Application number : 11-012980

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 21.01.1999

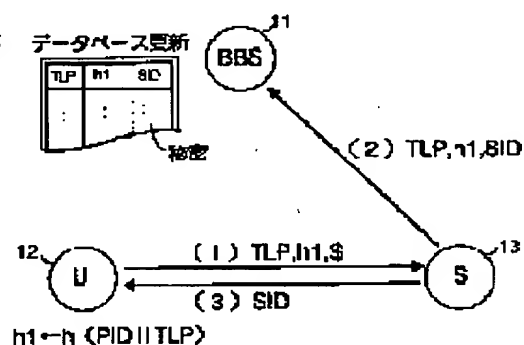
(72)Inventor : MORITA HIKARI

(54) METHOD AND DEVICE FOR PARTICIPATION TYPE LOTTERY

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent a sponsor from swindling winning money by the padding-out and to prevent a seller from embezzling a bet by generating hash values, for which the identifier and bedding pattern of a user are linked, with a hash function and requesting registration to a shop system while pairing these values.

SOLUTION: A user U generates a hash value $h1=h(PID/TLP)$ with a hash function (h) from PID/TLP, for which information PID for identifying an individual and a bedding pattern TLP are linked at a user system, and requests the registration to a shop system 13 while pairing TLP and $h1$. The shop system 13 generates an identifier SID, transmits the SID to the user system 12 and transmits TLP, $h1$ and SID to a bulletin board system BBS 11. The bulletin board system BBS 11 manages TLP, $h1$ and SID in a data base while pairing them.



LEGAL STATUS

[Date of request for examination]

26.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-215255

(P2000-215255A)

(43) 公開日 平成12年8月4日 (2000.8.4)

(51) Int.Cl. ⁷	識別記号	F I	テマコト (参考)
G 0 6 F 19/00		G 0 6 F 15/28	B 5 B 0 4 9
// G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 G 5 J 1 0 4
			6 6 0 E 9 A 0 0 1

審査請求 未請求 請求項の数9 O L (全 8 頁)

(21) 出願番号 特願平11-12980

(22) 出願日 平成11年1月21日 (1999.1.21)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 森田 光

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74) 代理人 100066153

弁理士 草野 卓 (外1名)

Fターム(参考) 5B049 BB11 BB37 BB46 CC39 EE03

EE05 FF03 FF04 GG04 GG07

GG10

5J104 AA07 KA01 KA03 KA05 NA05

NA12 NA36 PA00 PA12 PA17

9A001 EE02 EE03 JJ25 JJ76 KK60

(54) 【発明の名称】 参加型くじ方法及びその装置

(57) 【要約】

【課題】 安全性が高く、高速処理が可能で、主催者の当りくじ水増し、販売店の賭け金着服、ユーザのにせ当選金請求を排除する。

【解決手段】 ユーザUはその識別子P I Dと賭けパターンT L Pとの連結に対するハッシュ値 $h1 = h(P I D \parallel T L P)$ を求め、 $h1$ とT L Pとお金を販売店Sへ送り、Sよりその識別子S I Dを受領し、Sは $h1$ 、T L Pの登録を掲示板BBSに対し行う、BBSはT L P、 $h1$ 、S I Dを対としてデータベースで管理する。Uは $h1$ の部分情報 $h1^*$ とT L PをBBSへ送り問い合わせ、一致したものがデータベースにあれば、 $h1$ を返し、なければUはS I Dを根拠に異議を申し立てる。UはP I Dを金融機関Bに提示し、Bはその賭けた $h1$ と一致を確認して、当選金を支払う。

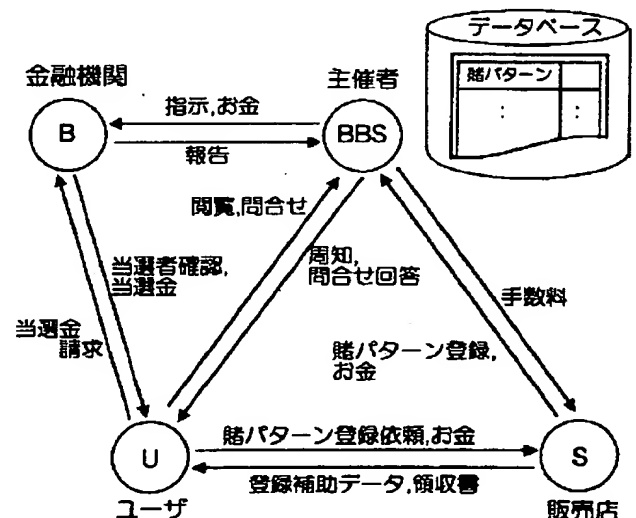


図1

【特許請求の範囲】

【請求項1】 掲示板装置と、ユーザの装置（以下ユーザ装置と記す）と、販売店装置と、金融機関装置とよりなり、

ユーザは上記ユーザ装置によりそのユーザを識別する情報PIDと賭けパターンTLPとを連結し、その連結PID||TLPからハッシュ関数hによってハッシュ値 $h_1 = h(PID || TLP)$ を生成し、賭けパターンTLPとハッシュ値 h_1 を対として販売店装置に登録依頼を行い、

販売店装置は上記登録依頼を受信すると、その販売店装置の識別子SIDを生成してユーザ装置に送信すると共に受信した賭けパターンTLPとハッシュ値 h_1 とを掲示板装置へ送信し、

掲示板装置は受信した賭けパターンTLP、ハッシュ値 h_1 を対としてデータベースに管理し、複数のユーザからの賭けパターンTLPが寄せられたら、その集計情報を公開し、

当選したユーザは掲示板装置に示された結果に従って、ユーザ装置により識別子PIDを示して金融機関装置に対して当選返戻金を請求し、

金融機関装置は当選返戻金請求を受けると、当選パターンが賭けパターンTLPであり、それに賭けられたハッシュ値 h_1 が、受信識別子PIDから作られていることを確認して、当選返戻金をユーザへ渡すことを特徴とする参加型くじ方法。

【請求項2】 請求項1記載の方法において、ユーザはユーザ装置により、上記ハッシュ値 h_1 の部分情報 h_1^* と賭けパターンTLPを掲示板装置へ送信して自らの賭けパターンTLPが存在することを問い合わせ、

この問い合わせを受けた掲示板装置は、問い合わせた賭けパターンTLP及び部分情報 h_1^* と一致するものがデータベース中に在れば、そのハッシュ値 h_1 をユーザ装置へ返送し、一致するものがなければそのことをユーザ装置へ返送し、

一致するものなしの返送を受けたユーザ装置のユーザは掲示板装置と販売店装置に対して識別子SIDを根拠に異議申し立てをすることを特徴とする参加型くじ方法。

【請求項3】 請求項1記載の方法において、販売店装置は上記登録依頼を受信した際に、販売店装置の識別子SIDを掲示板装置へ送信し、

掲示板装置は識別子SIDとハッシュ値 h_1 を連結し、その連結SID|| h_1 に対するハッシュ値 $h_2 = h(SID || h_1)$ を生成し、ハッシュ値 h_2 を上記賭けパターンTLP、ハッシュ値 h_1 に対としてデータベースに管理し、

ユーザはユーザ装置により、受信した識別子SIDとハッシュ値 h_1 を連結し、その連結SID|| h_1 に対するハッシュ値 $h_2 = h(SID || h_1)$ を生成し、そのハ

ッシュ値 h_2 の部分情報 h_2^* と賭けパターンTLPを掲示板装置へ送信して自らの賭けパターンTLPが存在することを問い合わせ、

この問い合わせを受けた掲示板装置は、問い合わせた賭けパターンTLP及び部分情報 h_2^* と一致するものがデータベース中に在れば、そのハッシュ値 h_2 をユーザ装置へ返送し、一致するものがなければそのことをユーザ装置へ返送し、

一致するものなしの返送を受けたユーザ装置のユーザは掲示板装置と販売店装置に対して識別子SIDを根拠に異議申し立てをすることを特徴とする参加型くじ方法。

【請求項4】 請求項1乃至3の何れかに記載の方法において、

掲示板装置は賭けパターン及びハッシュ値の公開リストに対し、掲示板装置の秘密の署名鍵で署名を生成し、その署名を上記公開リストに付けることを特徴とする参加型くじ方法。

【請求項5】 請求項1乃至4の何れかに記載の方法において、

ユーザ装置は上記ユーザ識別情報PIDに対しハッシュ値 $h(PID)$ を求め、このハッシュ値 $h(PID)$ と賭けパターンTLPを連結し、この連結 $h(PID) || TLP$ を上記識別情報と賭けパターンの連結とし、当選したユーザは識別子としてハッシュ値 $h(PID)$ を金融機関装置へ送り、

金融機関装置は賭けられたハッシュ値 h_1 が受けとったハッシュ値 $h(PID)$ から作られていることを確認し、その確認ができると、ユーザはPIDを金融機関装置へ示し、賭けられたハッシュ値 h_1 が示されたPIDから作られていることを確認して当選返戻金をユーザへ渡すことを特徴とする参加型くじ方法。

【請求項6】 参加型くじ方法に用いられるユーザ装置であって、

ユーザ識別子PIDなどを記憶する記憶部と、

入力手段と、

上記入力手段により入力された賭けパターンTLPと上記ユーザ識別子PIDとを連結する連結手段と、

上記連結したユーザ識別子PIDと賭けパターンTLPに対するハッシュ値 h_1 を求めるハッシュ関数手段と、販売店装置からのその識別子SID、掲示板装置からの応答などを受信する受信手段と、

上記ハッシュ値 h_1 、上記賭けパターンTLPを販売店装置へ、上記ハッシュ値 h_1 の部分情報 h_1^* 及び上記賭けパターンTLPを含む問い合わせを掲示板装置へそれぞれ送信する送信手段と、を具備するユーザ装置。

【請求項7】 参加型くじ方法に用いられるユーザ装置であって、

ユーザ識別子PIDなどを記憶する記憶手段と、

入力手段と、

上記入力手段により入力された賭けパターンTLPと上記ユーザ識別子とを連結する連結手段と、

上記連結したユーザ識別子PIDと賭けパターンTLPに対するハッシュ値h1を求めるハッシュ関数手段と、販売店装置からのその識別子SID、掲示板装置からの応答などを受信する受信手段と、

上記ハッシュ値h1と上記識別子SIDとを連結する手段と、

上記連結したハッシュ値h1と識別子SIDに対するハッシュ値h2を求める手段と、

上記ハッシュ値h1、上記賭けパターンTLPを販売店装置へ、上記ハッシュ値h2の部分情報h2*及び上記賭けパターンTLPを含む問い合わせを掲示板装置へそれぞれ送信する送信手段と、

を具備するユーザ装置。

【請求項8】 請求項6又は7記載のユーザ装置において、

ユーザ識別子PIDに対しハッシュ関数をかけてハッシュ値h(PID)を得るハッシュ関数手段を備え、

上記連結手段は、賭けパターンTLPと上記ハッシュしたユーザ識別子h(PID)とを連結する手段であり、上記ハッシュ関数手段はハッシュしたユーザ識別子h(PID)と賭けパターンTLPとの連結に対してハッシュをかける手段であることを特徴とするユーザ装置。

【請求項9】 請求項6乃至8の何れかに記載のユーザ装置において、

掲示板装置から受信した公開リストの署名を、公開鍵で検証する署名検証手段を備えることを特徴とするユーザ装置。

【発明の詳細な説明】
【0001】

【発明の属する技術分野】

この発明は、インターネットなど不特定多数の人々がアクセスできる環境下で、ゲームの結果などを対象にくじを投票し(賭け)公正に運用されるための参加型くじの方法及びそのユーザ装置に関する。ここで、参加型くじとは、競馬、競輪、競艇、ナンバーくじのたぐいのことであり、予め識別子が付され、くじが一意に定まっているものをユーザが購入するもの(例:宝くじ、宝くじ付年賀ハガキ)は、参加型くじの範囲には含まない。

【0002】参加型くじの重要な特徴は、予め参加者であるユーザが結果を予想し、その予想したパターンのくじを購入することにある。予想パターンとゲーム結果などが一致すれば、当選したとして当選返戻金(以下、当選金)が主催者から支払われる。

【0003】

【従来の技術】参加型くじのシステム構成を図11に示す。参加型くじを主催する主催者と、ユーザUと、販売店Sとよりなり、ユーザUが賭けパターンを予想してくじの購入を、販売店Sにお金を支払って行い、販売店S

から、そのくじと、領収書を受領する。販売店SはユーザUより希望賭けパターンを主催者へ報告すると共にお金を送り、主催者から手数料を受取る。ユーザUは当選くじを主催者に提示して当選金を主催者から受取る。

【0004】主催者と販売者の所属組織が同一の場合が多い。なお、主催者による賭け対象(ゲームなど)の情報は、自らと報道を通じて周知され、賭け結果も同様に周知される。ここでのセキュリティ上の問題点は次のとおりである。くじの偽造は、紙とそれに印刷される印字の複製困難性により決まる。主催者および販売者の不正、それら組織の内部犯行による不正は法律などにより防止される。

【0005】しかしながら、2000年開始が決まっているサッカーくじなど、新しい参加型くじを考える場合、多数の参加者を想定するので、販売者と主催者は別個と考えざるを得ないので内部犯行防止対策の強化が必要である。また、インターネットなど不特定多数がアクセスできるネットワーク環境が普及しつつあるが、紙と印刷からなるくじを見直す必要がある。閉じたシステムならば従来通りで同様のセキュリティが維持できるが、関わる人が多いオープンなシステムの場合、くじを作る印字機そのものよりも、主催者・販売者を行き交う情報そのものに、安全性の対策を講じたものとすべきである。

参加型くじシステムの定義

ここで、参加型くじシステムが扱う参加型くじシステムは次の様なものとする。

- ・賭けパターンの予想を対象とする。
- ・投票券(以下、くじ)は、1口単位に投票可。
- ・当選返戻金(以下、当選金)は、1口単位に与えられる。但し、当選金の額は、主催者が決定する。
- ・販売店の組織は複数、当選金は一金融機関が扱う。
- ・購入者の身分(年齢、銀行口座、等)の確認手段がある。
- ・決済手段は別にある。
- ・夜間販売禁止にできる。

参加型くじシステムの構成

この発明が前提とする参加型くじシステムの構成を図1に示す。各エンティティ(主体)は、次のような役割を分担する。主催者は、くじの運営に関する全責任を持つとし、集めたお金の管理を金融機関Bに委託し、くじの販売は販売者Sに委託する。また、自ら、くじのデータを蓄えるデータベースと、くじの条件や対象とするゲームの結果と当選報告などを周知し、ユーザからの問い合わせにも応じる掲示板BBSを運営する。金融機関は、くじの売り上げを主催者から預かり、当選くじを持っているユーザUの請求により、当選金を支払う。販売者はユーザからお金を貰って、ユーザの指示する賭けパターンを主催者に伝達する。くじを購入するユーザは、賭けるくじの条件などを、主催者の掲示板BBSなどから入

手し、くじの登録状況なども確認する。当選くじを持つユーザは金融機関に当選金を請求し、当選金を得る。なお、上記参加型くじシステムの定義のうち、夜間販売禁止は、システムの運用時間を設ければ解決するので以下の議論には含めない。

【0006】

【発明が解決しようとする課題】上記の様な構成を前提に以下の項目をこの発明が解決しようとする課題とする。

A. 主催者の、水増しによる当選金横取り詐欺を防止する。

B. 販売者の、主催者仲介をせず賭け金を着服する詐欺を防止する。

【0007】C. ユーザ（くじ購入者）の、にせの当選金請求を排除する。

D. 当選者のプライバシーを確保すると共に、他人のなりすましを防止する。

【0008】

【課題を解決するための手段】この発明によれば、ユーザはユーザ装置により、そのユーザの識別子PIDと賭けパターンTLPを連結し、その連結したPID||TLPに対するハッシュ値 $h1 = h(PID || TLP)$ をハッシュ関数hによって生成し、TLPとh1をペアとして販売店装置に登録依頼し、販売店装置はその識別子SIDをユーザ装置へ送ると共に、TLPとh1とSIDを掲示板装置へ送る。掲示板装置は受信したTLPとh1とSIDをペアとしてデータベースで管理し、ユーザ装置からh1の部分情報 $h1^*$ とTLPを掲示板装置へ送って、データベースに自らの賭けパターンTLPが存在することを問い合わせ、この時、掲示板装置はTLPと $h1^*$ が一致するTLPとh1があれば、そのh1を返し、自分の賭けパターンが自分のハッシュ値h1と一緒に存在しなければ、ユーザは掲示板装置及び販売店装置に対してSIDを根拠に異議申立てをする。掲示板装置はその集計情報を公開し、当選したユーザは掲示板装置により示された結果に従い、金融機関に対して当選返戻金を請求し、金融機関は当選パターンがTLPであり、それに賭けられたハッシュ値h1がユーザから渡された情報PIDから作られたことを確認してから、ユーザに当選金を渡す。

【0009】主催者の掲示板装置により次のような時系列の管理を行う。

Phase I 参加型くじの告示

ー試合とその賭け方の周知。

Phase II 経過処理

ー統計情報の公開、登録データの更新。

【0010】一個別問い合わせ回答（ユーザの登録確認）。

ー夜間は販売店と示し合わせて休業。

Phase III 投票確定（試合（ゲーム）の前に締切）

Phase IV 当選の案内（払戻し条件、等）

上記A～Dの課題に対応して、以下の様な手段を導入する。

【0011】一、（A対策）試合開始前の賭条件確定の為、掲示板は公開情報ファイル全体に“随時デジタル署名を付け公開”する。

二、（B、C対策）登録した自分のくじ（ハッシュ値）を問い合わせの為に“部分ハッシュ”を使用する。

三、（D対策）当選者のプライバシー保護と内部犯行ガードの為、個人情報“2重以上のハッシュ”で当選金手続き時の問い合わせに呼応する。

【0012】

【発明の実施の形態】参加型くじシステムの定義により、クレジット、電子マネー、またはデビットカード等で実現される。ここではどのようにするかの手法は述べない。このとき、ネットワーク上に存在する、掲示板装置BBS、販売者装置、ユーザ装置は次の様な関連をもって運用される。なお、金融機関Bとその他のエンティティBBSおよびUとの関係は、必ずしもネットワークで接続されている必要はない。とりわけ、当選金の支払処理は、オフラインを前提に以下の条件を進める。

Phase I 参加型くじの告示

ー掲示板装置BBSより、試合とその賭け方を周知させ、ネットワーク上に存在する多数のユーザU（必ずしもくじを買うことを必須としない）がこれを参照する。

Phase II 経過処理（販売など）

ーユーザUはそのユーザ装置によりネットワーク上で販売者Sの装置との間でくじを購買し、

ー販売者Sからその販売者装置により掲示板装置BBSにくじの登録を依頼し、

ー掲示板装置BBSは、くじの登録状況から、登録データの更新をするとともに統計情報を公開する。

【0013】ーユーザUよりそのユーザ装置により掲示板装置BBSへのくじ登録に関する個別問い合わせがあるとその回答をする（ユーザの登録確認）。

ー夜間などは販売者と示し合わせて、販売を休止する。

Phase III 投票確定（ゲーム（試合）の前に締切）

ー掲示板装置BBSはデータベースの中身を凍結する。

Phase IV 当選の案内（払戻し条件、等）

ー掲示板装置BBSから、当選の案内、支払条件の案内をする。

記号の凡例

・個人識別情報：PID

ー一意のもの。例；銀行口座番号であり、対象とするゲームや対象の勝敗引きわけの賭けパターン毎に変化させるための乱数エリアを持つ。

・賭けパターン情報：TLP

ー主催者側が設定し、対象ゲーム毎に区別可能とされる。

- ・連結: $X \parallel Y$
- $X \parallel Y$ は、 X の次に Y を並べることを示す。
- ・ハッシュ関数: $h()$
- $h1 \leftarrow h(PID \parallel TLP)$ は入力 $PID \parallel TLP$ のハッシュ値を $h1$ に代入することを示す。
- ・部分ハッシュ情報: h^*
- h^* はハッシュ値 h の一部分の値を示す。
- ・電子署名: $sSKa(X)$
- $s1 \leftarrow sSKa(X)$ は a さんの秘密の署名生成鍵 SKa で X に対して署名生成した署名を $s1$ に代入すると読む。

【0014】— $sSKa(X)$ は a さんの公開の署名検証鍵 PKa で X に対して署名検証でき、正しい署名生成鍵 SKa と X から生成された署名は有効と判断できる。従って、異なる署名生成鍵や入力 X の署名の場合、無効と判断される。— お金: \$ 電子的な金銭取引決済の流れを \$ シンボルで表す。

第一の実施例

掲示板装置 (BBS) 11、ユーザ U の装置 (ユーザ装置) 12、販売店 S の装置 (販売店装置) 13、金融機関 B の装置 (金融機関装置) 14 からなるシステムにおいて、図2に示すようにユーザ U はユーザ装置 12 により個人を識別する情報 PID と賭けパターン TLP より、 PID と TLP を連結した $PID \parallel TLP$ からハッシュ関数 h によってハッシュ値 $h1 = h(PID \parallel TLP)$ を生成し、 TLP と $h1$ をペアとして販売店装置 13 に登録依頼し、販売店装置 13 は識別子 SID を生成するとともに、ユーザ装置 12 には SID を、掲示板装置 BBS 11 には TLP と $h1$ と SID を送信する。

【0015】掲示板装置 11 は、 TLP と $h1$ と SID をペアにデータベースに管理し、図3に示すようにユーザ装置 12 によりユーザ U が上記 $h1$ の部分情報 $h1^*$ と TLP を掲示板装置 11 へ送信することで、上記データベースに自らの賭けパターン TLP が存在することを問い合わせたとき、掲示板装置 BBS は TLP と $h1^*$ がデータベース中の TLP ならびに $h1$ の一部と一致すれば、 $h1$ をユーザ装置 12 に返す。一方、自分の賭けパターンが自分のハッシュ値 $h1$ と一緒に存在しないときはそのことをユーザ装置 12 へ回答し、 U は BBS と S に対して、 SID を根拠に異議申し立てをする。これは、上記第二の手段“部分ハッシュ”の使用のことである。

【0016】なお、前記問い合わせに対して、 Yes か No だけで答えたとしても、答えに信ぴょう性がないので $h1^*$ を送信し、 $h1$ を回答することにしている。掲示板装置 BBS 11 は、複数のユーザから多数の TLP が寄せられたら、その集計情報を公開する。当選したユーザ U は、掲示板装置 BBS 11 により示された結果に従い、金融機関 B に対して図4に示すように情報 PID を渡し当選返戻金を請求し、金融機関 B はその装置 14

で、当選パターンが TLP であり、それに賭けられたハッシュ値 $h1$ が、 U から渡された情報 PID から作られることを確認してから、そのユーザ U に当選返戻金を渡す。

第二の実施例

第一の実施例で、ユーザ装置より $h1$ の部分情報 $h1^*$ を送って問い合わせを行ったが、第二の実施例では図5に示すように、 SID を $h1$ と SID の連結 $SID \parallel h1$ に対するハッシュ値 $h2 = h(SID \parallel h1)$ の部分情報 $h2^*$ について問い合わせる。この場合は、掲示板装置 11 でハッシュ値 $h2 = h(SID \parallel h1)$ を作って、 TLP と $h2$ と $h1$ と SID をペアとしてデータベースで管理する。

第三の実施例

第一の実施例では掲示板装置 11 のデータベースのうち、 TLP と $h1$ に関するリストを公開したが、第三の実施例では、図6に示すようにその公開リスト情報に関して、掲示板装置 11 が秘密の署名鍵 SK_{BB} で署名して公開する。これは、上記、第一の対策手段である。

第四の実施例

第一の実施例においてはユーザ装置 12 により、個人情報 PID と賭けパターン TLP より、 PID と TLP を連結した $PID \parallel TLP$ からハッシュ関数 h によってハッシュ値 $h1 = h(PID \parallel TLP)$ を生成した。この代わりに第四の実施例では図7に示すように、個人情報 PID のハッシュ値 $h(PID)$ と TLP を連結した $h(PID) \parallel TLP$ からハッシュ関数 h によってハッシュ値 $h1 = h(h(PID) \parallel TLP)$ を生成する。

【0017】ユーザ U が当選したとき、金融機能 B は図8に示すように当選パターンが TLP であり、それに賭けられたハッシュ値 $h1$ が、ユーザ U から渡された情報 $h(PID)$ から作られることを確認することを第一段階の確認とし、第二段階で PID 自身を渡して確認させる。この実施例は、上記第三の手段“2重以上のハッシュ”を用いることである。

【0018】図8で示した例は、2重ハッシュの場合であるが、金融機関 B が出張所、支店、本店と階層に分かれている場合、例えば3重ハッシュにし、問い合わせの階層が上る度に、よりハッシュが掛かってないハッシュに落として照合する。また、ハッシュ値多重では、 $h(h(PID \parallel TLP') \parallel TLP)$ 、 $h(h(h(PID \parallel TLP'') \parallel TLP') \parallel TLP)$ の様に、付加的な情報 TLP' 、 TLP'' を掲示板装置の指示の下、安全性を強化することができる。

【0019】上述したユーザ装置 12 の機能構成を図9に示す。記憶部 21 には識別子 PID の他、識別子 SID 、ハッシュ値 $h1$ 、署名検証用公開鍵 PK_{BB} などが記憶される。キーボードなどの入力手段 22 により賭けパターン TLP などを入力することができ、連結部 23 で PID と TLP が連結され、その連結はハッシュ関数部

24でハッシュ値 $h1$ が求められ、 $h1$ 、 TLP は送信部25より販売店装置へ送られる。またハッシュ値 $h1$ の部分情報 $h1^*$ と TLP が送信部25により掲示板装置へ送られ、問い合わせが行われる。受信部26にて販売店装置から SID を受信し、また、掲示板装置から公開リスト署名を受信し、公開リスト署名は署名検証部27にて公開鍵 PK_{BB} により検証される。

【0020】第二の実施例の場合は、 SID と $h1$ とが連結部28で連結され、その連結に対しハッシュ値 $h2$ がハッシュ関数部29で求められ、その $h2$ の部分情報 $h2^*$ と TLP が送信部25より掲示板装置へ送られて問い合わせが行われる。またくじの購入ごとに PID に乱数を付加する場合は、乱数生成部31から乱数 R を生成し、これを連結部23へ入力して、 PID と連結されればよい。

【0021】 PID をハッシュして用いる場合の例を図10に示す。記憶部21の PID を必要に応じて連結部32で乱数 R と連結し、その連結 $PID \parallel R$ に対するハッシュ値 $h(PID \parallel R)$ をハッシュ関数部33で求め、このハッシュ値 $h(PID \parallel R)$ と TLP を連結部23で連結し、その連結に対するハッシュ値 $h1$ をハッシュ関数部24で求める。その他は図9の場合と同様である。

【0022】

【発明の効果】上記各種実施例によれば、安全性が高く、速度性能において電子署名よりも効率の良いハッシュ関数をくじに用いることで、参加型くじシステムを構築することが出来る。また、くじを購入するユーザ個人にとっては、ハッシュ関数の計算の他は、ハッシュ値や

SID を控えておく程度ですむ。従って、ハッシュ関数は、街頭や喫茶店（サイバーカフェ）にある公共端末やネットワーク接続のパソコンで生成してもらい、控えとして、紙にメモするか、プリンタから印字する環境で構築できる。従来とは異なり、仮にこの控えが盗まれたり複製されても、個人情報 PID が前提であるのでこれを知らなければ、他人が得てもなんら意味を持たないからである。

【0023】掲示板装置の公開リスト署名を、ユーザの一部の有志がチェックすることにより、試合（ゲーム）結果が明らかになった後に主催者が当りくじを水増しするのを妨げることができる。ユーザが掲示板装置に問い合わせをすることにより、販売店での購入金着服に対するチェックをすることができる。

【図面の簡単な説明】

【図1】この発明の参加型くじシステムの構成を示す図。

【図2】くじ購買の手順を示す図。

【図3】登録確認の手順を示す図。

【図4】当選金受領の手順を示す図。

【図5】 SID による登録確認の手順を示す図。

【図6】登録簿署名の例を示す図。

【図7】くじ購買（2重ハッシュ関数利用）の他の手順を示す図。

【図8】当選金受領（2重ハッシュ関数利用）の他の手順を示す図。

【図9】ユーザ装置の機能構成例を示す図。

【図10】ユーザ装置の機能構成の他の例を示す図。

【図11】従来のシステムを示す図。

【図1】

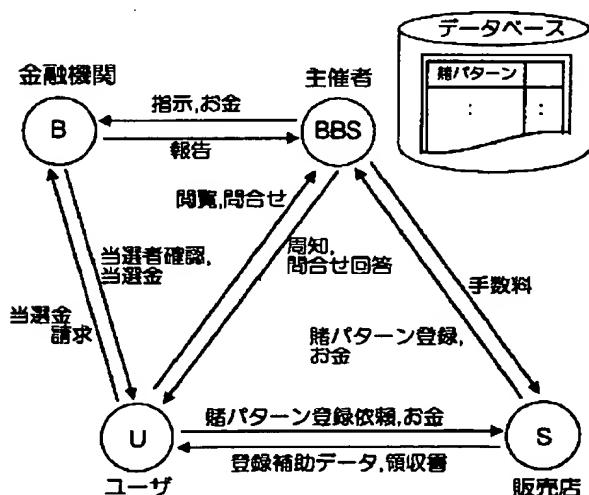
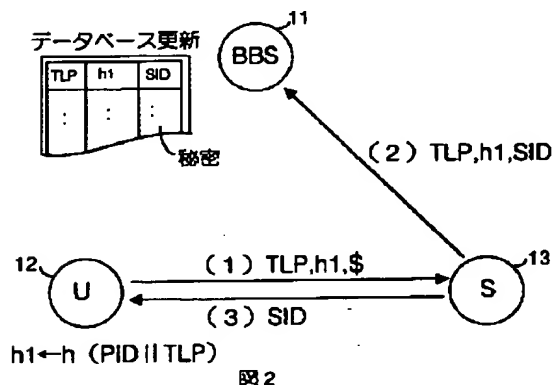


図1

【図2】



【図3】

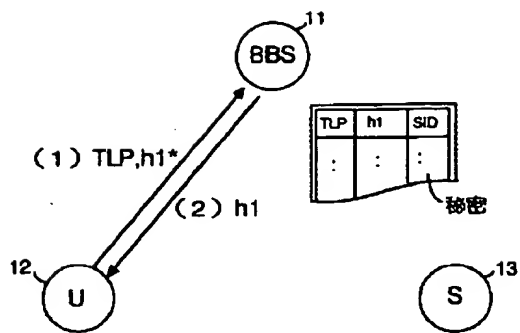


図3

【図4】

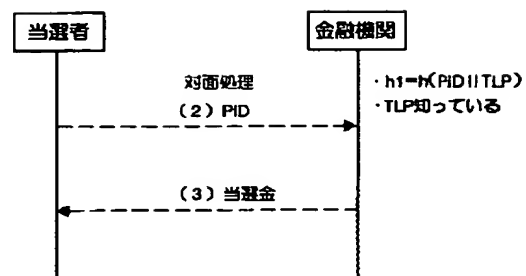


図4

【図5】

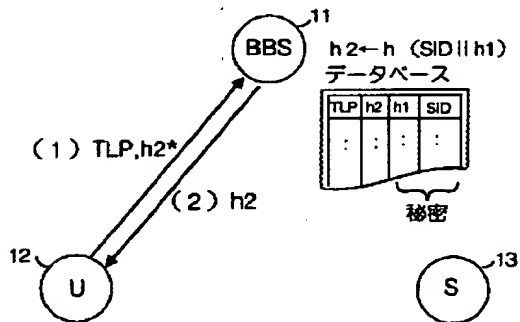


図5

【図6】

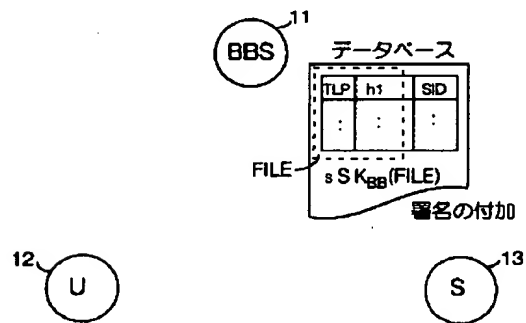


図6

【図7】

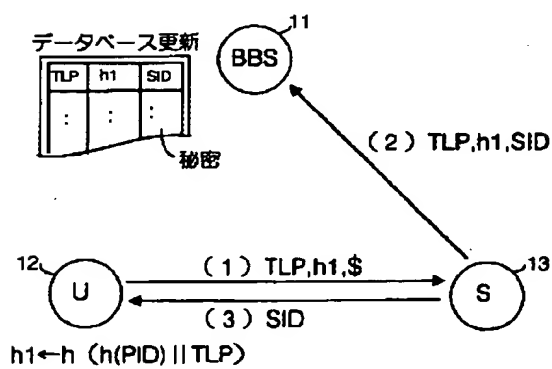


図7

【図8】

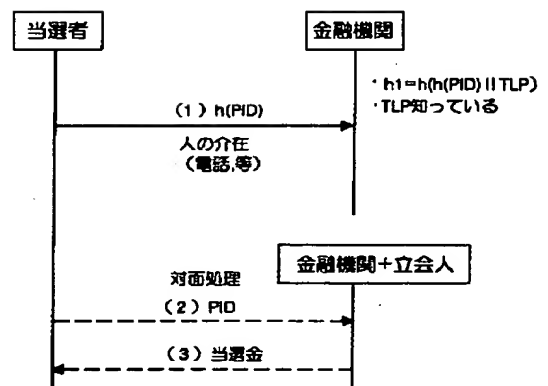


図8

【図9】

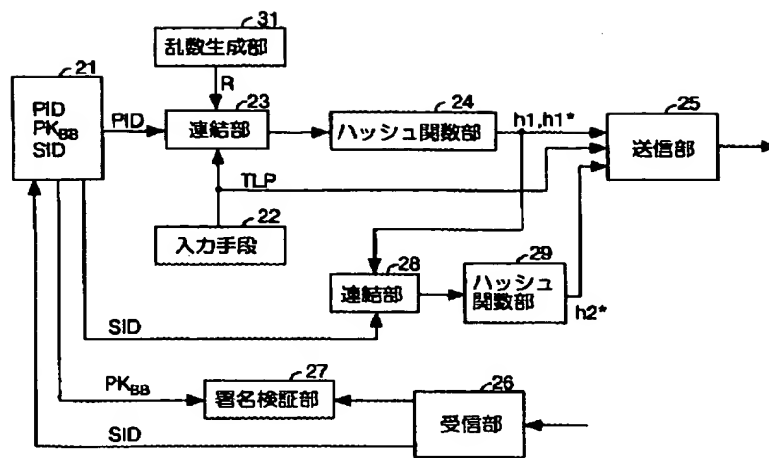


図9

【図10】

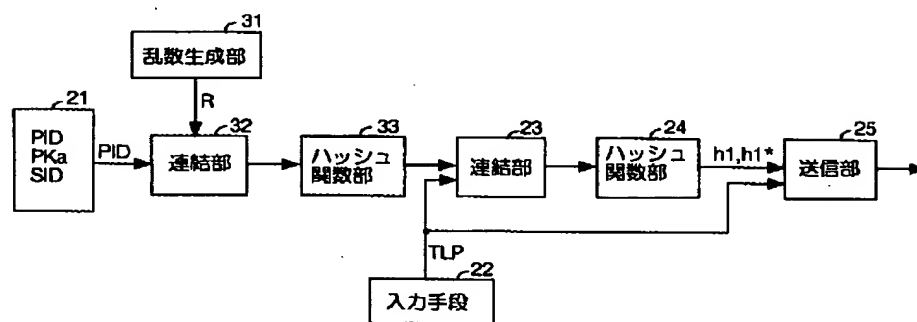


図10

【図11】

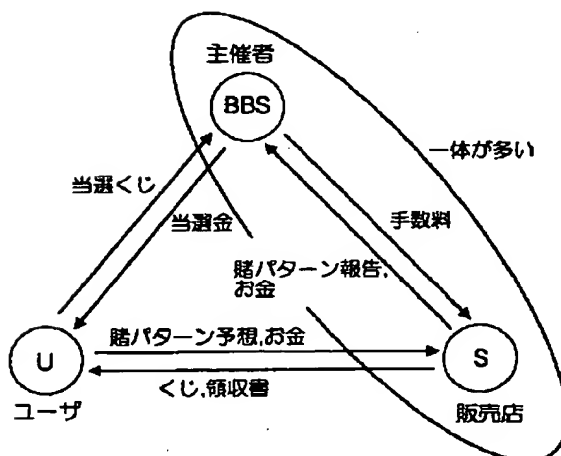


図11